Air Force/DoDIIS Security Certification (AFDSC)

AFC2ISRC/INY (OL-F)
AIR INTELLIGENCE AGENCY
DSN 969-3661/6346

This Briefing is Classified:
UNCLASSIFIED

OVERVIEW

- **What We Do**
- **DoDIIS C&A Guide**
- **Joint DoDIIS**
- **The MSRTM**
- **Test Procedures**
- **Test Reports**
- **Testing Concerns**
- **Questions**

What We Do

We perform security certification testing in accordance with the Director of Central Intelligence Directive (DCID) 6/3 on Special Compartmented Information (SCI) Intelligence Mission Applications (IMAs) that are assigned to the AF DoDIIS Executive Agent (DExA) by way of a *comprehensive* assessment of technical and non-technical security features.

Service Certifying Organization

DoDIIS Certification and Accreditation Guide paragraph 2.4 states that the SCO will:

- **Ensure each system under consideration meets all relevant security requirements for system operation specified in DCID 6/3**
- **Provide security technical and policy guidance to requesting parties**
- **Perform security testing and evaluations on new and modified Information Systems**
- **Grant IATO for Information Systems pending final decision by the DAA based upon favorable results from security testing**

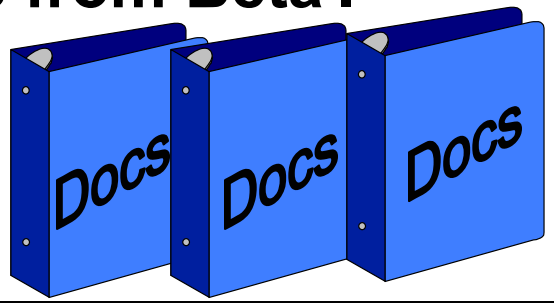
JDCSISSS

- Documentation review process:
  - JDCSISSS paragraph 2.3.4.1

  Time Line for Certification Activities outlines the 90 day period for Security documentation

  - SSAA 90 days from Beta I
  - SRTM 60 days from Beta I
  - Test Procedures 60 days from Beta I

  These documents can be a show stopper.



The Master SRTM

Master Security Requirements Traceability Matrix listed in the DoDIIS C&A Guide is a cut and paste document.

- **Protection Level, Integrity and Availability (H,M or B) is chosen and all other category requirements are deleted**
- **Controlled Interface is left in if it is applicable**
- **All other security requirements are left in**
- **Validation determination must be decided**
  - **I = Inspection (i.e. external markings)**
  - **A = Analysis (i.e. Backup procedures)**
  - **T = Test (i.e. log on/off, auditing etc.)**
  - **D = Demonstration (i.e. maintenance procedures)**

This forms the basis for everything we do!!

Test Procedures

Test procedures are developed for *all* SRTM requirements that indicate validation markings of "T"

- **Test procedures should be scenario-based encompassing all relative security requirements**
  - **I&A testing will show all I&A (log on/off), JDCSISSS (lock out & password), and AUDIT (session control) requirements.**
- **Some tests are done multiple times since it requires the same functions in order to get deeper into the application**

If a test can be done, then it should be done.

Security Test Reports

BETA I

- Accomplish ST&E and route test report recommendations to PMO with cc to DMB, SYS-4 and DExA.
- Any Cat I or II findings will require close-out actions before any recommendation to proceed to Beta II is given
  - Could possibly effect Beta II timeline

BETA II

- Same as Beta I above. Recommendation to Field will be given when there are no Category I or II findings
- Beta II Test site will get an IATO if it ***really is*** an operational site and there are no significant Site-related findings

Test Environment

Concerns

- Test sponsor should be available at the beginning of each day to ensure security clearances are available for SCIF entry
- A Systems Administrator(s) to properly configure and administer the test
  - have full rights to the network
  - needs to be available during the entire test time frame
  - have a flexible schedule and be dedicated for our use
- Test location(s) should provide adequate space and equipment for all testers and support staff to conduct business
- Priority should be given over day-to-day operations
- Test site and PMO should have better communications for a successful test to be conducted

SUCCESS = COMMUNICATION = SUCCESS

Contact

- **Phone Numbers:** DSN - 969-3661

  COMM - (210) 977-3661

- **Websites**

INTELINK

HTTP://WWW.AIA.IC.GOV/USAF/AFSCO

HTTP://WWW.AIA.IC.GOV/HOMEPAGES/ISS/INFOPROTECT/PIA/SCE/INDEX.HTML

SIPRNet

HTTP://WWW.AIA.KELLY.AF.SMIL.MIL/HOMEPAGES/ISS/INFOPROTECT/AFSCO/

NIPRNet

HTTPS://WWW.AIAWEB.AIA.AF.MIL/HOMEPAGES/690ISS/PI/PIA/INDEX.HTML


EIGHTH AIR FORCE
AIR INTELLIGENCE AGENCY
8 Seconds
AIR COMBAT COMMAND
8-Teen Hours